PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2001-134491**
(43)Date of publication of application : **18.05.2001**

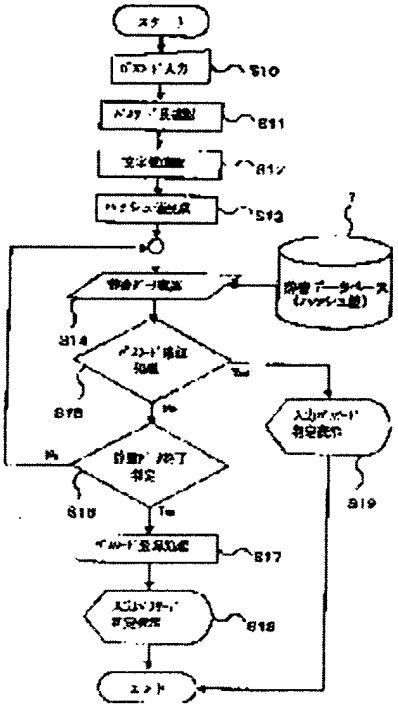
(51)Int.CI. G06F 12/14

(21)Application number : **11-312877**
(22)Date of filing : **02.11.1999**

(71)Applicant : **MITSUBISHI ELECTRIC CORP**
(72)Inventor : **CHOKAI KYOICHI**

(54) SYSTEM FOR SUPPORTING SELECTION OF PASSWORD

(57)Abstract:
PROBLEM TO BE SOLVED: To confirm whether or not an inputted password can be reasoned from an entry word included in a dictionary or the individual information of a user, and to register the password only when safety is confirmed.
SOLUTION: This system is provided with a password length confirming equipment for inspecting whether or not the length of the character string of an inputted password is within a set range, a kind of character confirming equipment for inspecting whether or not the kind of characters used for the password is the set kind of characters, a hash value generator for generating a hash value from the password, a dictionary data base for preliminarily storing the has value of the entry word, and a password confirming equipment for deciding whether or not the hash value of the password whose password length is confirmed and whose kind of characters is confirmed is compared with the hash value stored in the dictionary data base, and for deciding whether or not this hash value is matched with the stored hash value of the entry word, and for registering the has value of the password when they are not matched with each other.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] Only when this invention was described in more detail about the password decision support system for [in an information processor] supporting safe password selection, it checks whether the inputted password is safe and a safe thing is checked, it relates to the password decision support system which performs processing registered as a password.
[0002]
[Description of the Prior Art] Drawing 13 is a system concept view for explaining the conventional password decision support system. The keyboard for 1 inputting the terminal of an information processor and 2 inputting a password in drawing 13 The password length check machine which checks whether the character string of the password which 3 inputs, and 4 are as the length of the inputted password having specified beforehand, The character kind check machine which checks whether 5 includes the character kind which the inputted password specified beforehand, The hash value generation machine for generating a hash value from a password, since 6 saves the inputted password, 9 is the storage for saving the hash value of the generated password, and the above-mentioned password length check machine 4, the character kind check machine 5, and the hash value generation machine 6 constitute the control function of the control section (CPU) which a terminal 1 does not illustrate.
[0003] Next, operation concerning the above-mentioned composition is explained with reference to the flow chart shown in drawing 14 . In case a new user is registered into the terminal 1 of an information processor, it is required to set up the password for specifying the user. The new password 3 is inputted using a keyboard 2 (Step S10). It is checked whether the inputted password 3 is in the range of the string length which the password length set up beforehand in the password length check machine 4 (Step S11). Here, about the password of the string length outside a setting range, it warns of it being an unsuitable password to a registrant, and directs to redo the input of a password.
[0004] A check of that password length is in the range of a setting string length checks [next] whether with the character kind check vessel 5, the inputted password sets up beforehand and includes the character kind (Step S12). Here, about the password which does not fill a setting range, it warns of it being an unsuitable password to a registrant, and directs to redo the input of a password.
[0005] A check of including the character kind to which the password was set beforehand performs [next] processing which generates the hash value of the inputted password with the hash value generation vessel 6 (Step S13).
[0006] Password registration processing for memorizing the generated hash value to storage 9 at the end is performed (Step S19).
[0007] As mentioned above, in the conventional information processor, generally the user specification method using the password as a means for specifying the user who uses it is performed, and important data and the important program which are memorized by the information processor with the password are protected.
[0008]
[Problem(s) to be Solved by the Invention] However, although it is checking whether it is within limits set up beforehand about the number of characters, character classification, etc. of a password in the conventional password decision support system, it is not checking at all about the character string of a password itself. Therefore, a character string which is simply guessed to others was also registered as a password.
[0009] Moreover, a password decode attack called the dictionary attack which is the decode method of guessing others' password by comparing the hash value of data to the dictionary data of the character string contained in the dictionary with the hash value of the password registered when that malicious steals the others' password in recent years is delivered, and when language which is indicated by the dictionary is used as a password, a password will become clear easily.
[0010] Furthermore, when personal information, such as a birth date, is used for a password, an attack which decodes a password is also delivered from the personal information, and a password will make those malicious clear easily. Consequently, the damage which it is unlawfully invaded by the terminal 1 of an information processor, and the theft of important data and the important program which are accumulated is carried out to it, or is destroyed has occurred.
[0011] After performing processing which checks whether this invention can be guessed from the personal information of a keyword or a user that the password which was made in order to cancel the trouble concerning the conventional example mentioned above, and was inputted is contained in a dictionary, only when a safe thing is checked, it aims at obtaining the password decision support system which can be registered as a password.

check vessel 5 is included (Step S12). When the password which the user inputted does not include the character kind set up beforehand, a user is notified of that and the display it is directed that redoes the input of a password is performed.
[0021] The hash value which is the form for which it was suitable when the password inputted by the user with the hash value generation vessel 6 when the password which the user inputted included the character kind set up beforehand was accumulated is generated from the password.
[0022] Next, processing of the password check machine 8 concerning the form 1 of operation is explained. The password check machine 8 compares the hash value of the password into which the hash values of a keyword were collected (Step S14), and the hash value and user of the collected keywords inputted them from the dictionary database 7, and the conformity judging to which the character string which suits the hash value of a password checks whether it exists in the hash value of the keyword which the dictionary database 7 holds is performed (Step S15).
[0023] Next, it checks whether the data collection from the dictionary database 7 is completed (Step S16), and if it has not ended, it is carried out by returning to Step S14 and collection of the data from the dictionary database 7 continuing. On the other hand, if collection of the data from the dictionary database 7 is completed, it will shift to Step S17 and not suiting the hash value of the keyword which dictionary data have will make clear the hash value of the password which the user inputted. When not suiting becomes clear, it will be said that the password which the user inputted is suitable as a password, and processing which registers the hash value of the password inputted at Step S17 to storage 9 is performed. And the purport and user who registered the password inputted at Step S20 are notified.
[0024] On the other hand, in the above-mentioned step S15, when the hash value of a password and the hash value of the keyword which the dictionary database 7 holds suit, in Step S19, it displays on the inputted password, the purport that the keyword of the dictionary database 7 suited, and a user, and it is notified that the inputted password is disqualified as a password.

[0025] By doing in this way, it becomes possible to select and register a safe password to a dictionary attack, and the analogy of the password which used the dictionary by the malicious person becomes difficult.
[0026] That is, according to the form 1 of the above-mentioned implementation, it can check that it is that by which the character string of the password is not used for the keyword of a dictionary at the time of registration of a password, and it can verify at the time of registration that it is the safe password which is not guessed from the malicious others, the resistance over a dictionary attack can be verified beforehand, and only a satisfactory password can be registered.
[0027] Form 2. drawing 3 of operation is the block diagram showing the password decision support system concerning the form 2 of operation. In drawing 3 , the same portion as the form 1 of operation shown in drawing 1 attaches the same sign, and the explanation is omitted. As a new sign, 10 is a user personal information database which comes to accumulate personal information beforehand, and is set in the form 2 of this operation. the password check machine 8 Judge whether it suits with the character string contained in the personal information by which the character string of the password with which the password length check with the password length check machine 4 and the character kind check with the character kind check machine 5 were made was accumulated at the user personal information database 10, and when not suited It is made as [perform / the conformity judging based on comparison with the hash value generated with the hash value generation vessel 6 of the password concerned, and the hash value accumulated at the dictionary database 7].
[0028] Next, operation of the password decision support system concerning the gestalt 2 of operation which becomes with the composition shown in drawing 3 is explained with reference to the flow chart shown in drawing 4 and drawing 5 . The user who uses a terminal 1 newly is specified, and when registering the password for forbidding access from other than a specific person to the information accumulated at the terminal 1, Step S10 or operation of S12 is performed like the gestalt 1 of operation shown in drawing 2 . That is, it is checked whether the password which the password was inputted using the keyboard 2 (Step S10), and was first inputted by the password length check machine 4 is within the limits of the string length of the password set up beforehand (Step S11). When the string length set up beforehand is out of range, a user is notified of that and the display it is directed that redoes the input of a password is performed.
[0029] When the string length of the inputted password is within the limits of the string length set up beforehand next, it is checked whether the character kind to which the password which the user inputted is beforehand set with the character kind check vessel 5 is included (Step S12).
[0030] Next, processing of the password check machine 8 concerning the form 2 of operation is explained. The password check machine 8 performs processing which judges whether the character string contained in the password inputted as the character string which performs processing which collects personal information, such as a user, for example, a birth date, who is going to register the password from the user personal information database 10, and a personnel number, (Step S20), and is contained in the collected personal information suits (Step S21).
[0031] When the character string of the password which the character string contained in personal information and the user inputted in this step S21 suits, it shifts to Step S23, displays on the inputted password, the purport that personal information suited, and a user, and notifies that the inputted password is disqualified as a password. On the other hand, when the character string of the password which the character string contained in personal information and the user inputted does not suit, it becomes clear that bus WORD is not guessed from personal information, and processing is handed over by the following step S22. The hash value which is the form for which it was suitable when the password inputted by the user was accumulated with the hash value generation vessel 6 is generated from the password.
[0032] After that, as shown in drawing 5 , Step S14 or S19 is performed like the form 1 of operation. That is, the password check machine 8 compares the hash value of the password into which the hash values of a keyword were collected (Step S14), and the

without using a hash value.
[0044] Form 5. drawing 9 of operation is the block diagram showing the password decision support system concerning the form 5 of implementation of this invention. In drawing 9 , the same portion as the form 1 of operation or the composition in 4 attaches the same sign, and the explanation is omitted. The password into which the user inputted 12 as a new sign, and the personal information check machine which performs processing which personal information has, and which compares a birth date and a personnel number, for example, 13 is network networks, such as the Internet for connecting with a terminal 1 with two or more dictionary databases 7 of an external information processor, and is set in the form 5 of this operation. It is made as [use / two or more dictionary databases 7 which other information processing terminals connected through the network network 13 as a dictionary database 7 hold].
[0045] Next, operation is explained. In the form 5 of this operation, the form 1 of operation or the difference from 4 is to use two or more dictionary databases 7 to which the dictionary database 7 to be used was connected with the network network 13. Others are the same as that of the form 1 of operation, or 4.
[0046] Thus, according to the form 5 of operation, by utilizing more dictionary databases 7, it becomes possible to select a safe password more severely and to register it to a dictionary attack, and the analogy of the password which used the malicious personal information and two or more malicious dictionaries by the person becomes difficult.
[0047] Form 6. drawing 10 or drawing 12 of operation is a flow chart for explaining operation of the password decision support system concerning the form 6 of implementation of this invention. Although the form 6 of this operation is equipped with the same composition as the form 4 of operation As shown in drawing 10 or drawing 12 shown as compared with drawing 7 or drawing 8 which is a flow chart concerning the form 4 of operation The number input process S24 of proposals which inputs the number of candidates of the character string of the password proposed from a system side to a user as processing of the password check machine 8, The character string to propose is collected. A password The random number character string generation processing S25 to generate, The number of proposals of the password which the user inputted It has further the number end judging processing S26 of proposals in which it judges whether it generated or not, the calculation password proposal value display processing S27 which displays the computed password for several proposal minutes, and the selection password input process S28 which inputs the password which the user chose from the proposed password ** assistant value.
[0048] Next, operation is explained using drawing 10 or drawing 12 . Processing which first receives from a user the number of candidates of the password proposed from a system to a user by the number input process S29 of proposals is performed. Here, an inputted number of passwords will be generated, and a user will choose and use a password from the inside. Next, processing which generates at random the character sequence of numbers proposed by the random number character string generation processing S25 is performed, and processing is passed to Step S11.
[0049] Dictionary end-of-data judging processing of Step S16 is the same as that of the form 4 of operation from password length check processing of Step S11. Processing which judges whether generation of the number of candidates of a password inputted by the number input process S29 of proposals in Step S26 after dictionary end-of-data judging processing of Step S16 was completed is performed. When the number of candidates of a password is insufficient, processing which returns to Step S25 and generates a password ** assistant value further is performed. When the number of candidates of a password reaches the number of proposals inputted by the number input process S24 of proposals, processing is handed over to Step S27.
[0050] At Step S27, display processing for proposing one or more computed password candidate values to a user is performed. At Step S28, processing which receives the password which the user chose from the password ** assistant value displayed at Step S27 is performed. The received password is changed into the hash value suitable for accumulating on a terminal 1 at Step S13 (referring to drawing 12), and processing which registers the hash value of a password into storage 9 at Step S17 is performed. Finally, a user is notified of the purport that the password was regularly registered at Step S18.
[0051] Thus, it becomes possible to use it, setting up the password with which safety was secured, without a user worrying about a setup of a safe password by making the candidate value of a password propose from a system side using random number character string generating processing.
[0052]
[Effect of the Invention] As mentioned above, in case the password inputted by the user is registered according to this invention, it can support registering only the password which has intensity to the dictionary attack on the password from those malicious by making it associate with the keyword registered into the dictionary.
[0053] Moreover, in case the password inputted by the user is registered, it can support registering only the password which has intensity to the attack using the personal information over the password from those malicious by making it associate with the character string contained in a user's personal information.
[0054] Moreover, by utilizing the thing containing the keyword of the text form which is generally circulating the dictionary data used for a check as it is, the change and renewal of dictionary data are attained simply, and it can support registering only the password which has intensity to the dictionary attack which used the newest dictionary data to the password from those malicious.
[0055] Moreover, by utilizing the thing containing the keyword of the text form which is generally circulating the dictionary data used for making it associate with the character string contained in a user's personal information in case the password inputted by the user is registered, and a check as it is The change and renewal of dictionary data are attained simply, and it can support registering only the password which has intensity to the dictionary attack which used the attack using the personal information over the password to the password from those malicious, and the newest dictionary data.
[0056] Moreover, it is supportable by connecting through a network network and making the keyword of the dictionary data of